UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,560	06/28/2001	Robert A. Jerdonek	020967-000210US	7904

20350 7590 11/24/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 11/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,560	JERDONEK, ROBERT A.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *26 DEC 02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed 28 June 2001, with acknowledgement of continuing filing date of 17 January 2001.

2. Claims 1-20 are currently pending in this application. Claims 1, 7, and 14 are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 14, 15, 16, and 20** are rejected under 35 U.S.C. 102(e) as being anticipated by Chang et al. U.S. Patent No. 6,715,082 (hereinafter '082).

As to independent claim 14, "A method for a verification server comprises: receiving a request for a one-time password from a client computer" is taught in '082 col. 3, lines 24-62;

"determining a one-time password, the one-time password being inactive" is disclosed in '082 col. 7, lines 22-61;

"communicating data comprising the one-time password to the client computer receiving user identification data from a user at the client computer" is shown in '082 col. 6, lines 42-51;

"verifying the user in response to the user identification data; and activating the one-time password when the user is authenticated" is taught in '082 col. 7, lines 55-60.

As to dependent claim 15, "wherein communicating data comprising the one-time password to the client computer comprises communicating via an external server via a secure communications channel" is shown in '082 col. 5, lines 29-44.

As to dependent claim 16, "wherein the one-time password is selected form the group: random, pre-determined, pseudo-random" is disclosed in '082 col. 2, lines 15-16.

As to dependent claim 20, "further comprising: receiving a verification request from a password-based security system, the verification request comprising a user login and the one-time password; determining whether the one-time password is activated; and approving the verification request when the one-time password is determined to be active" is shown in '082 col. 7, lines 43-60.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-5, 7, 8, 10, 11, and 12** are rejected under 35 U.S.C. 103(a) as being unpatentable over '082 in further view of Yatsukawa U.S. Patent No. 6,148,404 (hereinafter '404).

As to dependent claim 1, "A method for communicating passwords comprises: receiving at a server a challenge from a authentication server" is taught in '082 col. 3, lines 24-62 "comprises the step of the first server communicating with a second server to determine whether the OTP is currently valid"

"via a first secure communications channel" and **"communicating the challenge from the server to a client computer via a second secure communications channel" and "receiving at the server a challenge response from the client computer via the second secure communications channel"** is shown in '082 col. 5, lines 29-44 "The network 108 is network system comprising any number of devices 114a, 114b, 114c interconnect by one or more communications channels ... In certain embodiments, a firewall (not shown) such as the Cisco PIX Firewall, ... may be logically interposed between the network access server 104 and network 108";

"the challenge comprising at least a random password that is inactive" is disclosed in '082 col. 7, lines 22-61 "Alternatively, if the AAA server 126 determines that the user identification information has expired, at block 318" ("random password that is inactive" the OTP is the random password also described col. 2, lines 15-16 / inactive same as expired);

"wherein the random password is activated when the authentication server verifies the challenge response" is taught in '082 col. 7, lines 55-60 "Alternatively, if the CHAP or PAP password is correct, at block 334 the AAA server 126 sends a message to network access server 104 indicating that a session may be established with client 102 based on the received user identification information" (i.e. "random password is activated" is the same as allowing access

based on received user identification);

the following is not taught in '082:

"the challenge response comprising a digital certificate and a digital signature, the digital certificate including a public key in an encrypted form, the digital signature being determined in response to at least a portion of the challenge and the private key; and communicating the challenge response from the server to the authentication server via the first secure communications channel" however '404 teaches "an authentication method for authenticating an authentication requester by using a public-key enciphering scheme in response" in col. 11, lines 8-39.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '082 method for communicating passwords to include a means to authenticate a user with public/private keys. One of ordinary skill in the art would have been motivated to perform such a modification to because as network communication improves a need exist to verify an entity utilizing electronic methods. As indicated by '404 (see col. 1, lines 15-32) "For instance, in a case where legal action is taken between business entities or between individuals, conventionally (or even now), a contract or the like is written on a physical document, signed, impressed with a seal, and if necessary, accompanied with a registration certificate of seal impression or a notary certificate by notary officials ... Technology in electronic data communication that safely substitutes the above action taken mostly on physical documents, is the network security technology ... the demands on network security technology are steadily increasing".

As to dependent claim 2, "wherein the client computer communicates the random password to a password-based security system, the password-based security system coupled to the authentication server" is taught in '082 col. 3, lines 24-62.

As to dependent claim 3, "wherein the password-based security system comprises a firewall" is shown in '082 col. 5, lines 29-44.

As to dependent claim 4, "wherein the public key and the private key are associated with an authenticated user" is disclosed in '404 col. 11, 8-39.

As to dependent claim 5, "wherein the private key is not associated with an authenticated user, and wherein the authentication server does not authenticate the challenge response" is taught in '404 col. 11, lines 8-39.

As to independent claim 7, "A method for a client computer comprises: receiving challenge data from a authentication server" is taught in '082 col. 3, lines 24-62 "comprises the step of the first server communicating with a second server to determine whether the OTP is currently valid";

"via a first secure communications channel" is shown in '082 col. 5, lines 29-44 "The network 108 is network system comprising any number of devices 114a, 114b, 114c interconnect by one or more communications channels ... In certain embodiments, a firewall (not shown) such as the Cisco PIX Firewall, ... may be logically interposed between the network access server 104 and network 108";

"the challenge data comprising a challenge and a password that is inactive" is disclosed in '082 col. 7, lines 22-61 "Alternatively, if the AAA server 126 determines that the

user identification information has expired, at block 318" ("random password that is inactive" the OTP is the random password also described col. 2, lines 15-16 / inactive same as expired); "receiving a user PIN" is taught in '404 col. 9, lines 35-36 "inspecting a code number or the like";

"recovering a private key and a digital certificate in response to the user PIN; sending the digital certificate to the authentication server via an external server, the digital certificate comprising a public key in an encrypted form; sending a digital signature to the authentication server via the external server, the digital signature being determined in response the challenge and the private key" is shown in '404 col. 11, lines 8-39 "an authentication method for authenticating an authentication requester by using a public-key enciphering scheme in response" in col. 11, lines 8-39.

"and thereafter sending a user login and the password to a password-based security system coupled to the authentication server, wherein when the authentication server verifies the digital signature, the password is activated" is disclosed in '082 col. 7, lines 22-61 "Alternatively, if the AAA server 126 determines that the user identification information has expired, at block 318" ("random password that is inactive" the OTP is the random password also described col. 2, lines 15-16 / inactive same as expired).

As to dependent claim 8, "wherein when the authentication server does not verify the digital signature, the password remains inactive" is shown in '082 col. 7, lines 51-55 "If the CHAP or PAP password is not correct, at block 330 the AAA server 126 sends a message indicating that a session may not be established".

As to dependent claim 10, "wherein recovering the private key and the digital certificate in response to the user PIN comprises: recovering a private key associated with the user when the user PIN is correct; and generating a private key not associated with the user when the user PIN is incorrect" is disclosed in '404 col. 9, lines 35-55 "This is further developed in the use of IC card. First, an IC card it self verifies an individual who is about to use the IC card by requiring a code number, and when this verification succeeds, the authentication operation by the server is initiated via network. The server performs authentication processing using the IC card (i.e. entity such as an individual, verified by the IC card) by using the "knowledge" technique or "cipher" technique".

As to dependent claim 11, "further comprising manually entering the user login and the password to the client computer" is shown in '404 col. 9, lines 55-56 "a dedicated input/output device is required between the possession and client terminal".

As to dependent claim 12, "wherein the password is activated for a pre-determined amount of time" is disclosed in '082 col. 9, lines 25-30 "As inidicated above, a set of cached user identification information may be configured to expire after the expiration of a cache time-out value".

As to dependent claim 13, "wherein after the pre-determined amount of time, the password is inactivated" is taught in '082, col. 8, lines 5-10 "In addition, a cache time-out value is set to cause the user identification information to expire (to become invalid) after a certain period of time regardless".

7. **Claims 6 and 9** are rejected under 35 U.S.C. 103(a) as being unpatentable over '082 in further view of '404 in further view of Baskey et al. U.S. Patent No. 6,732,269 (hereinafter '269).

As to dependent claim 6, the following is not taught in the combination of '082 and '404: **"wherein the first secure communications channel is selected from the group: secure socket layer and secure HTTP"** however '269 shows "When a connection is made, the transaction server 50 waits for a message over alternate port X and when a message is received the client information is extracted from the received message (block 224) and the extracted client identification information is matched with a corresponding message from the persistent SSL connection 44 (block 226). Such a match may be made by, for example, incorporating message identification information into the SSL message and the message transmitted over the second connection 60 such that, if the message identification information matches, then the message received over the second connection 60 is a match with the message received over the persistent SSL connection 44. The client identification information and the information content of the message are provided to the transaction server application 54 (block 228). As will be appreciated by those of skill in the art, the client identification information may include the user's name, location, organization, organizational unit, e-mail information, privileges and any other information defined by the administrator who issues the client's digital ID (X.509 V1 and V3 certificate format). The client identification would not need to be limited to the contents of the digital certificate. The SSL proxy could also map the certificate to other security credentials such as a Kerberos Pass Ticket or Resource Access Control Facility (RACF) login id" in col. 9, lines 39-64.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '082 and '404 a method for communicating passwords by authenticating a user with public/private keys to include a means to utilize a secure socket layer. One of ordinary skill in the art would have been motivated to perform such a modification to. because as network communication improves a need exist to maintain with security communication standards available. As indicated by '269 (see col. 1, lines 13 et seq.) " In communications between a client and a server, it is often beneficial to provide increased security. One mechanism for providing increased security is through the use of the Secure Socket Layer (SSL) protocol. FIG. 1 illustrates a conventional SSL connection between a client 10 and a server 12. As seen in FIG. 1, the client 10 communicates directly with the server 12 utilizing the SSL connection".

As to dependent claim 9, "wherein the password-based security system comprises a server selected from the group: a firewall and a VPN Gateway" is shown in '269 col. 5, lines 38-57 "other forms of secure connection may be utilized, such as, for example, a Virtual Private Network (VPN) tunnel, Internet Protocol Security (IPSEC)".

8. **Claims 17-19** are rejected under 35 U.S.C. 103(a) as being unpatentable over '082 in further view of '404.

As to dependent claim 17, the following is not taught in '082 **"wherein the user identification data comprises a digital signature"** however '404 teaches "an authentication method for authenticating an authentication requester by using a public-key enciphering scheme in response" in col. 11, lines 8-39.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '082 method for communicating passwords to include a means to authenticate a user with public/private keys. One of ordinary skill in the art would have been motivated to perform such a modification to because as network communication improves a need exist to verify an entity utilizing electronic methods. As indicated by '404 (see col. 1, lines 15-32) "For instance, in a case where legal action is taken between business entities or between individuals, conventionally (or even now), a contract or the like is written on a physical document, signed, impressed with a seal, and if necessary, accompanied with a registration certificate of seal impression or a notary certificate by notary officials ... Technology in electronic data communication that safely substitutes the above action taken mostly on physical documents, is the network security technology ... the demands on network security technology are steadily increasing".

As to dependent claim 18, "wherein the digital signature comprises a private key selected from the group: associated with the user, not associated with the user" is disclosed in '404 col. 11, lines 8-39.

As to dependent claim 19, "wherein verifying the user comprises verifying the user when the private key is associated with the user" is shown in '404 col. 11, lines 8-39.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Newport et al. U.S. Patent Application Publication No. 2004/0059952

Ha et al. U.S. Patent Application Publication No. 2003/0152254

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
03 November 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100